

# (12) UK Patent Application (19) GB (11) 2 329 497 (13) A

(43) Date of A Publication 24.03.1999

(21) Application No 9719874.1

(22) Date of Filing 19.09.1997

(71) Applicant(s)  
International Business Machines Corporation  
(Incorporated in USA - New York)  
Armonk, New York 10504, United States of America

(72) Inventor(s)  
Howard Shelton Lambert  
James Ronald Lewis Orchard

(74) Agent and/or Address for Service  
M J Jennings  
IBM United Kingdom Limited, Intellectual Property  
Department, Mail Point 110, Hursley Park,  
WINCHESTER, Hampshire, SO21 2JN,  
United Kingdom

(51) INT CL<sup>6</sup>  
G07F 7/10 , G06F 1/00 12/14

(52) UK CL (Edition Q )  
G4H HTG H1A H13D  
G4A AAP

(56) Documents Cited  
GB 2104696 A EP 0286094 A2 US 5285055 A  
US 4816653 A

(58) Field of Search  
UK CL (Edition P ) G4A AAP , G4H HTG  
INT CL<sup>6</sup> G06F , G07F

(54) Abstract Title  
Controlling access to electronically provided data or services

(57) The security of stored data and applications is improved by an access control system and method in which user keys for accessing the stored data/services (which keys are provided to users) are representative of the user's level of authority, such that there is no need to maintain a separate lookup table of user authority levels. This removes a potential security exposure from the system.

The user keys are advantageously hierarchical, including data for generating a plurality of different access keys for different access levels. The access keys may be decryption keys for encrypted data or application programs. The invention is applicable to SmartCard systems.

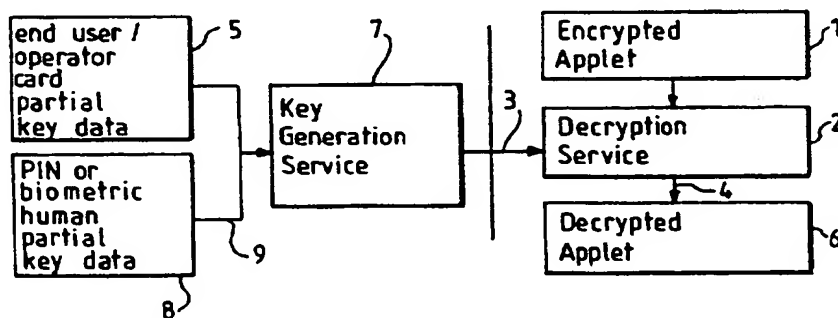
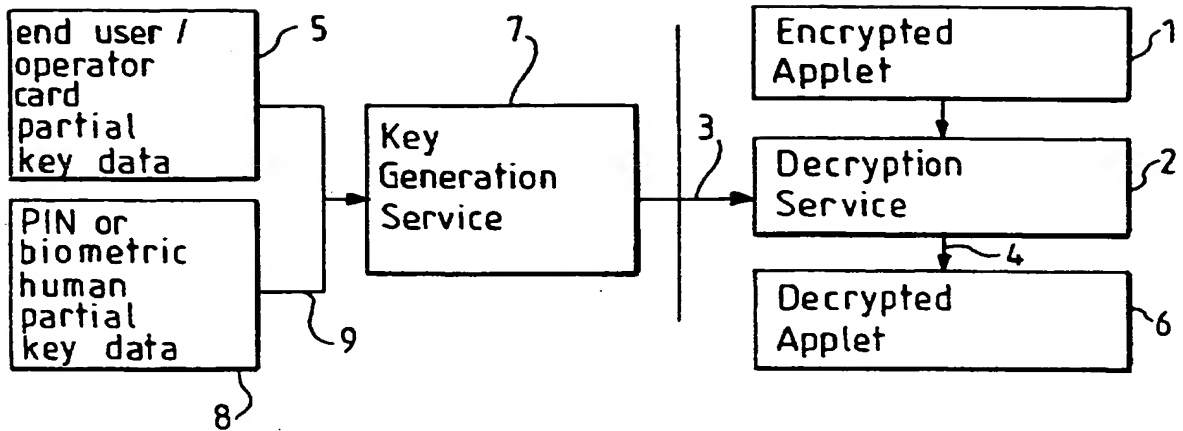
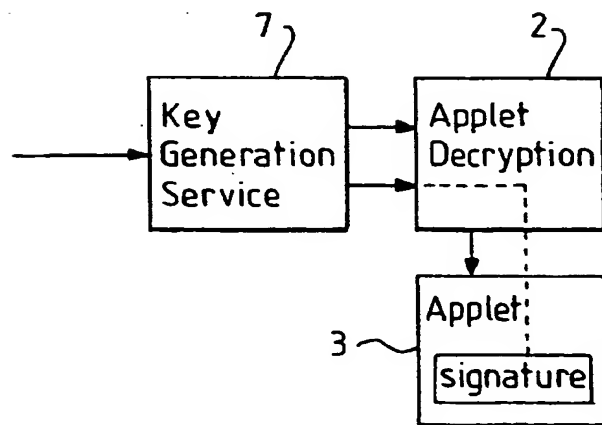
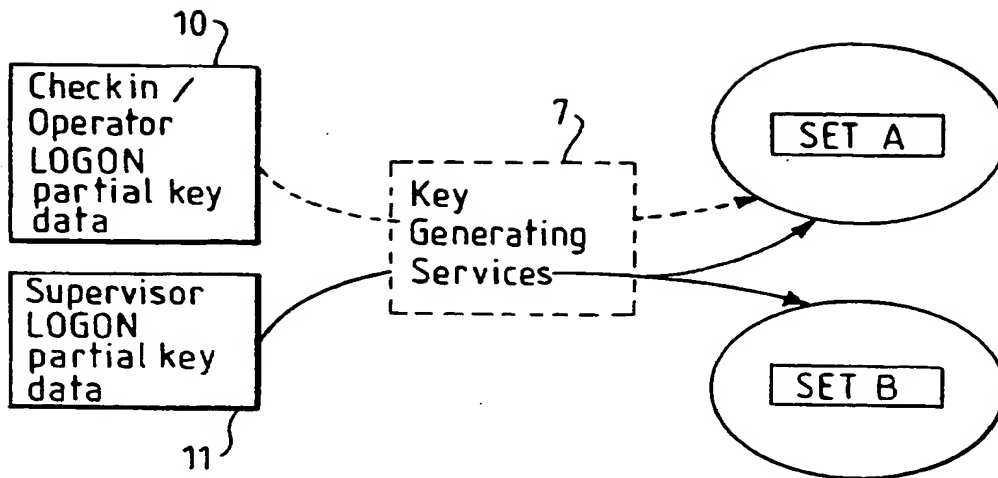
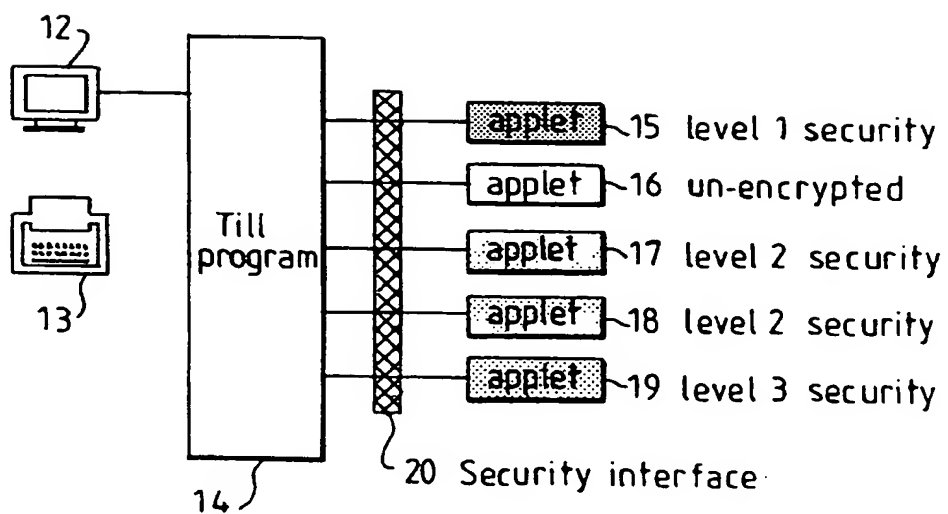
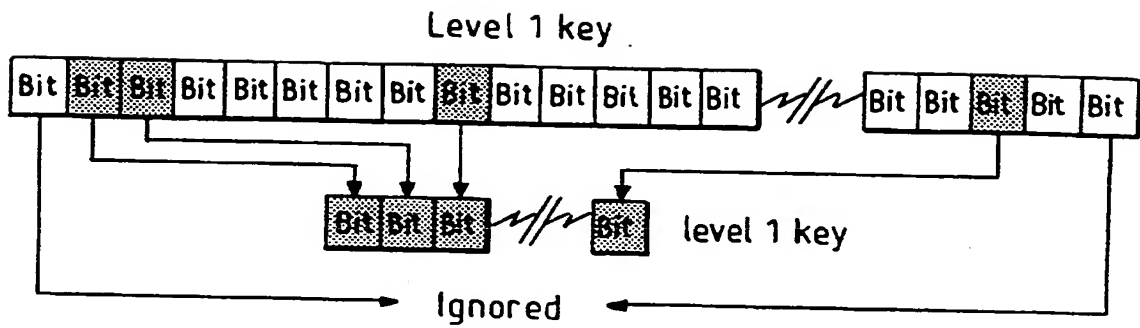
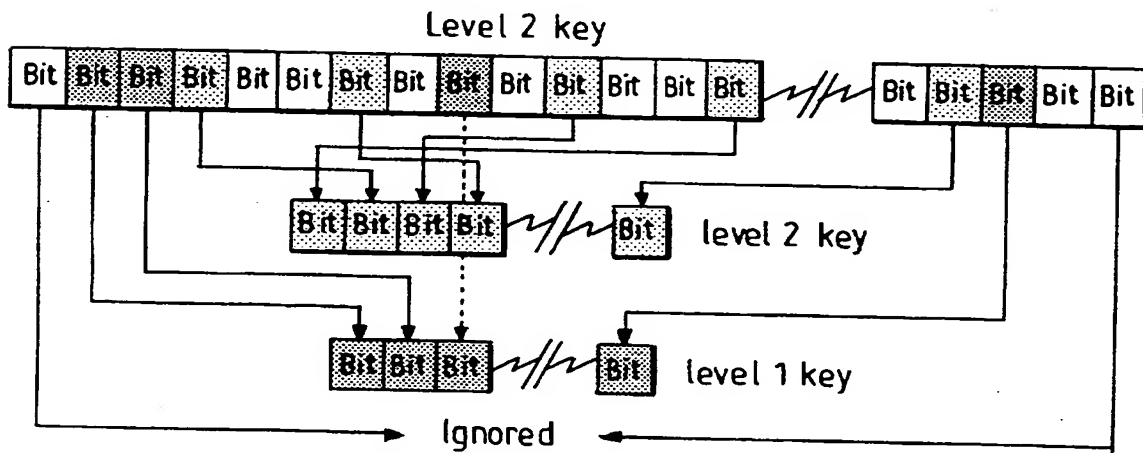
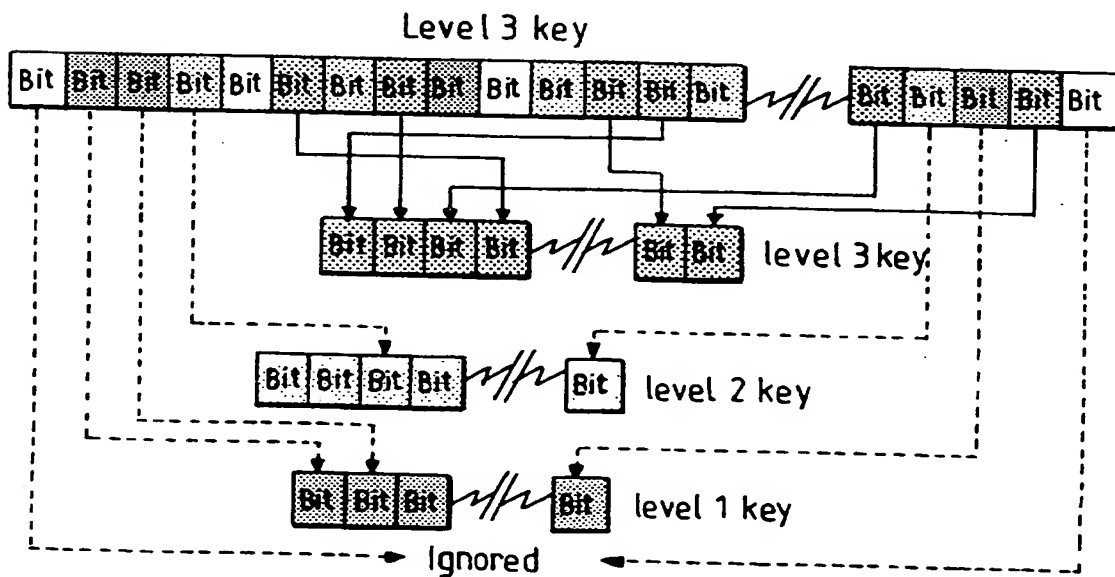


FIG. 1

GB 2 329 497 A

FIG. 1FIG. 2

FIG. 3FIG. 4

FIG. 5FIG. 6FIG. 7

METHOD FOR CONTROLLING ACCESS TO ELECTRONICALLY PROVIDED  
SERVICES AND SYSTEM FOR IMPLEMENTING SUCH METHOD

Field of the Invention

This invention relates generally to the control of access to stored data and/or electronically provided services.

Background of the Invention

An example of such a service is the dispensing of cash by an automatic teller machine (ATM). Access to facilities provided by the ATM are typically controlled by requiring a user to present a personalised plastic card carrying data on a magnetic stripe to a card reader associated with the ATM. The user is required to key in a personal identification number (PIN) which is used by the system to access data in the card which together with data held in the system relating to the user enables the system to determine whether the requested transaction should be authorised.

The principle has been considerably extended to many types of transactions including the purchase of goods in retail outlets, access to processes on computer networks and the provision of stockbroking services. As the sophistication of the services has increased so has the need for increased flexibility and security in the control of access. For example, it is important that providers of services through retail tills/terminals or ATM's are assured that such services may only be accessed by authorised end-users with a valid access card, at a valid till and, where appropriate, under the control of an authorised sales assistant or other operator. Applications providing services may be held on the system in an encrypted form requiring a decryption key to access them, and the decryption key is then only provided to identified authorised users when they present a valid access card. It is also desirable to provide an audit trail for each transaction to facilitate the detection of fraud and the settlement of any dispute that may arise from the transaction.

An improved form of plastic card, called the Smart Card, has been developed which by incorporating within it active data processing and storage facilities provides enhanced security and flexibility. Data and application programs can be made inaccessible until an authorised person

(as identified by personal information input by that person) presents their SmartCard. The present invention is suitable for use with SmartCards but is not limited thereto.

5           A problem arises when seeking to control access to application program modules where a number of different users are required to be allowed to access different sets of application modules. For example, in a retail environment, it may be desirable for all till operators to run certain applets associated with sales whereas only the store manager can  
10       access other applets associated with stock control or payroll. The conventional approach to this problem is for a computer LOG ON procedure to include identification of the user from user input data (and optionally additional data held on a token such as a SmartCard). A table lookup process then scans a static list to determine the access authority  
15       of the user, and the user is given access to certain applications according to their determined authority level.

          Such conventional systems relying on lookup tables of user authorities are vulnerable to breaches of security even if the  
20       applications themselves are held in a protected (e.g. encrypted) form if the list can be tampered with. An unauthorised person may seek to add themselves to the list or to change their authority level within the list.

#### 25       Summary of the Invention

          In a first aspect, the invention provides a data processing system including means for controlling user access to data or services, wherein data or application modules for providing the service are stored in a  
30       form which is inaccessible without an access key. Users are each allocated a specific 'user key' which is appropriate for their level of access authority. When a user requests access to stored data or requests a service for which stored software modules must be accessed, the data or modules are interrogated to identify their stored security access level.  
35       If the user key represents the required level of access authority an access key is generated from the user key for accessing that data or service.

          Since user keys include the data for generating access keys once a  
40       stored module has been interrogated, the user key directly determines the

user's authority level and so there is no need to rely on separate lists of user authorities. This represents a significant security advantage.

5       The generated user keys are preferably hierarchical keys which include data for generating an access key for each of a plurality of different access levels (that is, where the owner of the user key is authorised for more than one level). The access key is generated from the hierarchical user key after interrogating the requested data or software module to determine which of the possible access keys is required.

10       The access keys according to a preferred embodiment of the invention are decryption keys for accessing data or application modules stored in an encrypted form.

15       The user key may be dynamically generated when the user logs on to the system or it may be pregenerated and, for example, stored on a token such as a SmartCard. In a preferred embodiment of the invention, a user key is dynamically generated when a user presents a token and inputs personal data (for example a personal identification number or PIN, input via a keypad), combining these separate data portions to produce the key.

20       In a second aspect of the invention, there is provided a method for controlling user access to data or services via a computer system, including the steps of:

25       storing said data or services in a form accessible only under the control of one or more access keys;

30       providing users with a user key representing their authority level for accessing specific data or services; and

35       in response to a user request for access to said stored data or services, determining the access level of the requested data or services and, if the user's authority level as represented by the user key matches the determined access level, generating from said user key an access key for accessing said data or services.

40       In a third aspect of the invention, there is provided a security interface for a computer system for controlling user access to data or services stored on said system in a form accessible only under the control of one or more access keys, the security interface including:

means for generating a user key representing a user's authority level for accessing specific data or services; and

5 means, responsive to a user request for access to stored data or services, for determining the security access level of the requested data or services; and

10 means for generating from said user key an access key for accessing said data or services if the user's authority level as represented by the user key matches the determined access level.

15 The invention may be implemented as a computer program product comprising computer readable program code stored on a computer readable storage medium, the computer program code providing the functions for controlling access to stored data or services.

20 In a typical system the personal data relating to the user will be a personal identification (PIN) number and the data receiving means will be a simple keypad. However in a more advanced system the data may be developed from biometric data read by a reader adapted to recognise particular facial or other characteristics of the user such as fingerprint or hand geometry.

25 In order to provide an audit trail there may also be developed, at the same time as the generation of the access key, data identifying the end user, the token used and any operator involved, together with the date of the transaction and any other information required to establish an audit trail.

30 The system is preferably organised to operate under the control of an object orientated (OO) programming language and the services are stored in the form of encrypted object oriented "applets".

35 In a number of applications, particularly where transactions are performed in association with an operator or operators, it is desirable to make provision for access to processes according to the level of authority delegated to the operator or operators involved. In one embodiment of the invention, a set of applications is made available to all operators of check-out tills in a retail environment whilst a further set of applications is available only to supervisors. In another  
40 embodiment of the invention, different sets of applets may be decrypted



according to the authority of an operator as identified when the operator logs on to a particular terminal. In such a system, a hierarchy of access levels may be established by associating with each applet a level of access such that the applet is accessible only to operators or users able to satisfy the system that they have the appropriate access authority level.

In a preferred system embodying the invention provision is made for accepting smart cards. Advantage is taken of the processing and storage facilities available on the card to perform the key generation on the card itself and, where sufficient processing capacity is available, the decryption itself. The dynamic generation of the decryption key on the smart card provides the considerable security advantage that the personal information on the card relating to the user need never leave the card. Moreover further security advantages may be obtained by generating a key, or set of keys representative of a user's personal level of authority to access particular services, obviating the need to maintain a separate list of operators and their access authorities. Prior systems requiring such a list are vulnerable to breaches of security if such a list is tampered with.

In order that the invention may be well understood, preferred embodiments thereof will now be described by way of example, with reference to the accompanying drawings in which:

Fig. 1. shows a basic access control system embodying the invention.

Fig. 2. is a block diagram showing the manner in which an audit trail is developed in the system of Fig. 1.

Fig. 3. shows an embodiment of the invention providing two different levels of access according to the authority of the operator or user of a requested service.

Fig. 4. shows an embodiment of the invention providing a hierarchy of authority according to security levels allocated to various users or operators.

Figs. 5, 6 and 7 illustrate the development of different levels of decryption key in the embodiment of Fig. 4.

Referring to Fig. 1. there is shown in simplified form the basic features of a retail till or automatic teller terminal embodying the invention. An application store (1) is provided to retain in encrypted form those applications which the terminal may be called on to perform, according to the authority of users requesting the application. In a preferred system embodying the invention the applications take the form of object oriented "applets". Such "applets" may be stored in the terminal on a permanent or semi-permanent basis or may be erased and replaced from time to time from a central storage device according to the needs of the terminal. A decryption service module (2), typically a software module arranged to control a processing unit, is provided to decrypt a selected applet under the control of a decryption key provided over a bus (3). The decrypted applet is provided to a register (6) over a bus (4) to control operation of the requested service.

Partial key data (5) is read from a card presented by a user and supplied to a key generator (7). Personalised data such as a personal identification number (PIN) or biometric data is obtained from the user by a reader (8) which supplies this further data over a bus (9) for combination with the data (5) in the key generator (7) to develop a decryption key to be supplied to the decryption service (2) over bus (3).

The preferred system provides for access to be controlled using a smart card. When such a card is presented the key generation service is performed on the card using its processing and data storage facilities, minimising the amount of customer personal data supplied to the terminal and thus enhancing the security of the system. If sufficient processing and storage facilities are available on the card, the security of the system may be further enhanced by performing the decryption process itself using these facilities.

On power up, the till program invokes an applet controlling operator LOG ON. This applet requires the operator to insert his or her smart card and additionally to provide either PIN or biometric data. Partial data is read from the operator's card and combined with the PIN or biometric data supplied to provide an input to the key generator (7) enabling it dynamically to generate a key or keys permitting the decryption of applets.

The till program also invokes a LOG ON applet for each customer requesting a service, reading partial key data from his or her card and

collecting PIN/biometric data and providing this data as input to the key generating service.

When a service is invoked, for example if the operator initiates a payment, the applet controlling payment is invoked, and the decryption service (2) accesses the key generator which provides:

1. If authorised, a dynamically generated decryption key.
2. Data identifying the end user and the operator and their respective cards.

The decryption service then uses the decryption key to decrypt the applet to perform the requested service. The data identifying the end user and the operator is, as shown in Fig. 2, used to "sign" the transaction, for example by inserting a message authorisation code (MAC) into information sent to the server to which the till is attached. The latter may then log audit trail data for retention with details of the transaction.

In certain applications it may be required that only certain operators may access the till/terminal services, and that the services they can access, are limited to those pre-defined for the operator's authority level and for the business purpose of the till. It may additionally be required that certain operators having a higher level of authority, for example supervisors, may concurrently have access to a till or terminal. Fig. 3. shows an embodiment of the invention which addresses such requirements.

Referring to Fig. 3. there is shown a till/terminal environment with two sets of stored applets (A) and (B), set A being accessible to operators and supervisors of checkout tills and set B only available to supervisors. In the embodiment of Fig. 3. operator log on is controlled by a till program which determines according to business needs whether multiple log ons are permitted, and if so, permits only multiple log ons which conform to certain rules. For example the rule may require that only one valid operator is permitted with one valid supervisor, there being no other valid case of multiple log on.

In the embodiment shown in Fig. 3. partial key data from the till operator is read at (10), and corresponding data from the supervisor at

(11). The data is supplied to the key generator (7) to develop a key or keys which control the selection of an application applet from set A or set B or both according to the authority of the check-in operator.

Fig. 4. shows an embodiment which provides a number of levels of authority permitting only operators having a security level matching or exceeding a pre-determined threshold to execute a classified applet.

Referring to Fig. 4., a checkout terminal includes a display (12) and a console (13) operating under the control of a till program (14) resident in the terminal to process user initiated transactions involving various application modules or applets (15-19). Access to the applets by the till program is regulated by a security interface (20) which includes a key generator and decryption facilities as already described with reference to Fig. 1. As described with reference to Fig. 1., when a till operator logs on at the console with a personal smart card that stores their details together with a partial decryption key, the remainder of the key, for example a personal identification number (PIN) is entered at the console (13). The whole decryption key so derived defines the security level of the operator as described below.

In this embodiment the string of bits constituting the decryption key is processed using an algorithm which selects those bits which are to be used for a given security level. Preferably higher security levels include the bit pattern of the lower security levels, permitting a higher level decryption key to be used to decrypt a lower level applet. Figs. 5-7 provide examples of how the bits used for the security level keys may be inter-mixed in a final decryption key.

In the example shown there are four security levels, 0, 1, 2 and 3. Security level 0 is allocated to applets of such low security that no encryption is required. Level 1 is allocated to the lowest level of encryption, level 2 to a higher level of encryption which includes level 1 and level 3 to a still higher level which includes both levels 1 and 2.

When an applet is encrypted the following data is supplied:

- o a user key
- o a security level

o a master key

The key generator (7) in the security interface (20) operates in accordance with an algorithm which causes bit patterns to be generated which will be used to develop a user de-cryption key which is unique and specific to the user seeking access to an applet and an imbedded code included in the encrypted applet which identifies the security level allocated to that particular applet. Once the keys have been generated any encryption/decryption system may be used.

Figs. 5-7 illustrate the manner in which keys are developed in the security interface (20) for the various security levels.

Clearly for level 0, the associated applets are in plain language and no key is required. As shown in Fig. 5 the key generation algorithm is arranged to select a group of bits from the bit string developed from the data read by till program (14) when the user logs on. It will be appreciated that this is a simple example of how the algorithm may operate to select the various bits. In practice various bit transpositions or arithmetic operations may be used to generate the final key.

As shown in Fig. 6. a number of additional bits are selected which, together with the bits already selected for level 1, constitute the level 2 key. Similarly as shown in Fig. 7. further bits are selected to supplement those already selected for level 1 and level 2 to constitute the level 3 key.

The algorithm used to select the bits and the order in which they are re-combined may be different for each key level and may include bits selected from the lower level keys. Thus when a request is made for access to a particular applet the decryption algorithm uses the user key in conjunction with the security level encoded within the encrypted applet to determine the key level. The appropriate bit pattern is selected from the user key, thus permitting the appropriate decryption bit key sequence to be generated. Upon completion of the decryption a user identifier is inserted into the applet so that at execution time the applet can indicate the operator for whom it was decrypted.

While the invention has been described above in relation to transaction terminals it will be appreciated that it is applicable in any

situation where access is sought to processes or other potentially sensitive material in the course of a card initiated transaction. For example it may readily be applied to environments such as the Internet in which access is sought to software and may only be granted if the requestor is appropriately authorised.

## CLAIMS

1. A method for controlling user access to data or services via a computer system, including the steps of:

storing said data or services in a form accessible only under the control of one or more access keys;

providing users with a user key representing their authority level for accessing specific data or services; and

in response to a user request for access to said stored data or services, determining the access level of the requested data or services and, if the user's authority level as represented by the user key matches the determined access level, generating from said user key an access key for accessing said data or services.

2. A method according to claim 1, wherein said user key is an hierarchical key including data for generating an access key for each of a plurality of different access levels.

3. A method according to claim 1 or claim 2, wherein the storing step comprises storing data and/or application modules in an encrypted form and said generated access keys are decryption keys.

4. A method according to any one of the preceding claims wherein said user key is dynamically generated, in response to a user request initiated by presentation of a token by a user, from token data read from said token and personal data provided by the user.

5. A data processing system including means for controlling user access to data or services, the system including:

means for storing said data or services in a form accessible only under the control of one or more access keys;

means for generating a user key representing a user's authority level for accessing data or services; and

means, responsive to a user request for access to stored data or services, for determining the access level of the requested data or services; and

5 means for generating from said user key an access key for accessing said data or services if the user's authority level as represented by the user key matches the determined access level.

10 6. A data processing system according to claim 5, wherein said means for generating user keys is adapted to generate an hierarchical key including data for generating an access key for each of a plurality of different access levels.

15 7. A data processing system according to claim 5 or claim 6, wherein said means for storing includes means for encrypting said data or application modules providing said services and wherein said means for generating an access key comprises means for generating a decryption key.

20 8. A data processing system according to any one of claims 5 to 7 wherein said means for generating user keys comprises means responsive to a user request initiated by presentation of a token by a user, for dynamically generating a user key from token data read from said token and personal data provided by the user.

25 9. A security interface for a computer system for controlling user access to data or services stored on said system in a form accessible only under the control of one or more access keys, the security interface including:

30 means for generating a user key representing a user's authority level for accessing specific data or services; and

35 means, responsive to a user request for access to stored data or services, for determining the security access level of the requested data or services; and

means for generating from said user key an access key for accessing said data or services if the user's authority level as represented by the user key matches the determined access level.





The  
Patent  
Office

13

Application No: GB 9719874.1  
Claims searched: 1-9

Examiner: Mike Davis  
Date of search: 12 January 1998

**Patents Act 1977**  
**Search Report under Section 17**

**Databases searched:**

UK Patent Office collections, including GB, EP, WO & US patent specifications, in:

UK Cl (Ed.P): G4H (HTG), G4A (AAP)

Int Cl (Ed.6): G07F, G06F

Other:

**Documents considered to be relevant:**

Category	Identity of document and relevant passage	Relevant to claims
X	GB 2104696 A (AMERICAN DISTRICT TELEGRAPH)	1,5,9 at least
X	EP 0286094 A2 (CASIO)	"
X	US 5285055 (OONAKAHARA ET AL)	"
X	US 4816653 (ANDERL ET AL) eg col 5 ln 18 to col 6 ln 27	"

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.

